

REMARKS

This Amendment is fully responsive to the non-final Office Action dated August 27, 2008, issued in connection with the above-identified application. A petition for a one-month extension of time accompanies this Amendment. Claims 1-34 were previously pending in the present application. With this Amendment, claims 1-34 have been canceled without prejudice or disclaimer to the subject matter therein; and claims 35-62 have been added. Accordingly, claims 35-62 are all the claims presently pending in the present application. No new matter has been introduced by the new claims added. Favorable reconsideration is respectfully requested.

At the outset, to facilitate the Examiner's reconsideration of the present application, the Applicants have provided a substitute specification and a replacement abstract. The changes to the specification and abstract include minor editorial and clarifying changes. In addition to the substitute specification and replacement abstract, a "marked-up" copy of the original specification and abstract are also enclosed. No new matter has been introduced by the changes made to the specification and abstract.

In the Office Action, claims 1 and 6 have been objected to because of minor informalities. Specifically, the Examiner alleges that claim 1 is not the least restrictive claim because it consists of limitations recited in claims 7, 13 and 19; and claim 6 has terms that lack proper antecedent basis. The Applicants have canceled claims 1 and 6 rendering the above objection to those claims moot.

The Examiner is also reminded that 37 C.F.R. 1.75 (g) states that "the least restrictive claim should be presented as claim number 1 and all dependent claims should be grouped together with the claim or claims to which they refer to the extent practicable." Thus, the above language in 37 C.F.R. 1.75 (g) is considered a recommendation, not a requirement. Additionally, the Applicants assert that the new independent claims are the least restrictive claims in their respective grouping of claims. Moreover, the new claims have modified the original claim 6 to correct the antecedent basis issues identified by the Examiner. Withdrawal of the objection to the above claims is respectfully requested.

In the Office Action, claims 33 and 34 have been rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter. Specifically, the Examiner alleges that the claims are

directed to software *per se*, and lack any physical article or object that constitutes a machine or manufacture within the meaning of 35 U.S.C. 101. Claims 33 and 34 have been canceled thereby rendering the above rejection to those claims moot. Withdrawal of the rejection under 35 U.S.C. 101 is respectfully requested.

In the Office Action, claims 1, 2, 6-8, 12-14, 18-20 and 24-34 have been rejected under 35 U.S.C. 102(b) as being anticipated by Lotspeich et al. (U.S. Patent No. 6,118,873, hereafter "Lotspeich"); claims 3, 9, 15 and 21 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspeich in view of Ishiguro et al. (U.S. Publication No. 2001/044897, hereafter "Ishiguro"); and claims 4, 5, 10, 11, 16, 17, 22 and 23 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspeich in view of Masuda et al. (European Patent No. 0969667, hereafter "Masuda").

The Applicants have canceled claims 1-34 thereby rendering the above prior art rejections to the above claims moot. Additionally, the Applicants assert that the cited prior art fails to disclose or suggest all the features recited in at least independent claims 35, 41, 47, 53, 60, 61 and 62.

For example, claim 35 recites the following features:

"[a] copyright protection system comprising:

a recording apparatus configured to encrypt a content and to record the encrypted content;

a recording medium on which the encrypted content is recorded; and

a plurality of reproduction apparatuses, each of which is configured to read out and decrypt the encrypted content recorded on said recording medium,

wherein each of said plurality of reproduction apparatuses is one of either a first plurality of reproduction apparatuses which belong to a first category and hold plural device keys and information regarding generation of the plural device keys or a second plurality of reproduction apparatuses which belong to a second category and hold only one device key,

said recording apparatus is configured (a) to generate, for said plurality of reproduction apparatuses and based on a media key and the device key held by each of said plurality of reproduction apparatuses, a plurality of revocation data intended for revoking a device key held by a specific reproduction apparatus of a respective category, (b) to generate the encrypted

content which is the content encrypted based on the media key, and (c) to record the plurality of revocation data, the information regarding the generation of the device keys for generating the plurality of revocation data, and the encrypted content onto said recording medium,

the first plurality of reproduction apparatuses are each configured (a) to read out, from said recording medium, the plurality of revocation data corresponding to said first plurality of reproduction apparatuses, the information regarding the generations of the plural device keys, and the encrypted content, and (b) to decrypt the encrypted content based on the plurality of revocation data read out and the information regarding the generation of the plural device keys, and

the second plurality of reproduction apparatuses are each configured (a) to read out, from said recording medium, the plurality of revocation data corresponding to said second plurality of reproduction apparatuses and the encrypted content, and (b) to decrypt the encrypted content based on the plurality of revocation data read out.”

At least one or more of the above features of system of independent claim 35 are similarly recited in independent claims 41, 47, 53, 60, 61 and 62. Additionally, the features noted above are believed to be fully supported by the Applicants’ disclosure.

The copyright protection system (as recited in claim 35 and similarly recited in claims 41, 47, 53, 60, 61 and 62) addresses the disadvantages in the similarly prior art systems. More specifically, when the adding/updating of a device key is performed in a reproduction apparatus belonging to the first category, the recording apparatus generates, using a new device key, encrypted media key data (revocation data) corresponding to the reproduction apparatus belonging to the first category. On the other hand, the reproduction apparatus belonging to the first category holds plural device keys in advance and performs decryption by selecting the appropriate device key based on information regarding the generations of the device keys in the recording medium.

According to the copyright protection system of the present invention, it is possible to sequentially update a device key of the reproduction apparatus belonging to the first category (for which the danger of device key leakage is high), without affecting the second category for which the adding/updating of a device key is difficult. Thus, the copyright protection system of

the present invention produces the remarkable effect of enabling copyrights to be easily and reliably protected even when various reproduction terminals having different configurations are connected.

On the other hand, the cited prior art fails to disclose or suggest the above features and advantages of the copyright protection system of the present invention.

For example, Lotspiech discloses a system which, when an encryption leakage occurs from a user apparatus corresponding to the reproduction apparatus, disables non-encryption of a broadcast program in the user apparatus by replacing at least one of plural session numbers making up a session key block (corresponding to the "media key") with a dummy number.

Ishiguro discloses a technique for generating a session key using a hash coefficient; and Masuda disclose a technique for encrypting data using a scramble key K_s , the scramble key K_s using a real-time encryption key K_{w1} , and the real-time encryption key K_{w1} using a real-time master key K_{m1} .

However, Lotspiech, Ishiguro and Masuda (individually or in combination) fail to disclose or suggest anything regarding the ease of adding/updating a device key or that the danger of device key leakage is different for a plurality of reproduction terminals connected to a system. Furthermore, Lotspiech, Ishiguro and Masuda (individually or in combination) fail to disclose or suggest anything regarding a configuration for updating only the device key of a reproduction terminal for which the danger of device key leakage is high, without affecting a reproduction terminal for which updating of a device key is difficult.

Based on the above discussion, no combination of Lotspiech, Ishiguro and Masuda would result in, or otherwise render obvious, independent claims 35, 41, 47, 53, 60, 61 and 62. Moreover, no combination of Lotspiech, Ishiguro and Masuda would result in, or otherwise render obvious, independent claims 36-40, 42-46, 48-52 and 54-59 at least by virtue of their respective dependencies from independent claims 35, 41, 47, and 53.

In light of the above, the Applicants respectfully submit that all the pending claims are patentable over the prior art of record. The Applicants respectfully request that the Examiner withdraw the rejections presented in the outstanding Office Action, and pass the present application to issue.

Respectfully submitted,

Naoki YAMAMOTO et al.

/Mark D. Pratt/

By: 2008.12.29 10:45:23 -05'00'

Mark D. Pratt
Registration No. 45794
Attorney for Applicants

MDP/ats
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
December 29, 2008